How Quantum got Gamed

Faisal Shah Khan,
Department of Mathematics, Khalifa University, Abu Dhabi, UAE
faisal.khan@ku.ac.ae

Nour Abura'ed
College of Engineering and IT, Mohammed Bin Rashid Space Center (MBRSC) Lab,
University of Dubai, Dubai, UAE
noaburaed@ud.ac.ae

Since the 1960's, scientists have promised technologies working on the principles of quantum mechanics that can solve age-old problems facing the human civilization. For instance, consider the challenge of tamper-proof currency. Counterfeit currency can wreak havoc on an economy, most obviously in the form of uncontrollable inflation caused by large amounts of counterfeit currency circulating the economy. Uncontrolled inflation over-values the assets in a society or economy and negatively affects the cost and standard of living, and hence counterfeit currency is a relatively cheap but effective way to bring down a government from bottom-up. Much effort has therefore been put by central authorities throughout history into the development of tamper-proof currency, although prior to the 1960's all they could achieve in reality was tamper-resistant currency.

A common strategy adopted prior to the emergence of industry-based economics in the 18th century was to issue currency in the form of coins made of rare metals, typically gold or silver. This policy made counterfeiting a challenge simply because only the authorities had enough stores of these metals (due to their control over the police and armed forces). Unfortunately, this solution would consistently lead to economic deflation, making economic enterprise and growth difficult as only a limited amount of currency would circulate the vast majority of an economy (only those close to the authorities would get most of the gold and silver). Some authorities tried printing treasury-backed paper bills, such as the Tang dynasty in China in the 600's [1], but mostly for private bills of credit or exchange notes. And as this paper currency became more commonly used, inflation reared its ugly head, prompting a ban on paper currency in China circa 1455. Surely, counterfeiters got the best of this effort at easing deflation! More modern efforts in making tamper-resistant currency bills have of course been extremely successful; however, the prospect of a smart and dedicated counterfeiter finding a hack and reproducing even these currencies is ever present. Hence, the lynchpin that can hold the inflation-deflation dynamic in equilibrium is tamper-proof currency.

Until 1968, this lynchpin was beyond the reach of human knowledge and technological creativity. What was needed was a creative application of quantum physics, and Stephen Wiesner [2]. Wiesner, a quantum physicist, used the *truly* random nature of quantum physical systems as a solution to the problem of creating electronic tamper-proof currency. It is an often obfuscated fact that non-quantum physical systems only mimic randomness via chaotic properties (such as the number of wing flutters of a small group of humming birds) and their behavior may in fact be predicted with access to a suitably powerful computer and a careful enough analysis. On the other hand, certain physical properties of a quantum system are fundamentally inversely correlated, technically known as *conjugate pairs*, so that increasing the precision in acquiring information about one physical

property, such as the momentum of an electron, decreases the precision with which information about the other property, such as the position of the electron, can be gained. This feature of quantum physical systems is known as the Heisenberg uncertainty principle [3]. Wisener's quantum money utilized the Heisenberg uncertainty system to ensure, in principle, that a counterfeiting attempt would always fail. This is made possible by assigning serial numbers to the electronic currency bills. The value of each digit in the serial number is generated by following a protocol to gain precise information about one physical property of a conjugate pair in a quantum system. This means that even if a counterfeiter knows what the protocol is, he still has to guess, with a (true) 50-50 chance, which one of the two physical properties in the conjugate pair was used to generate the digit's value in the serial number. If he attempts to learn the value of the digit, half the time he will learn the value with exact precision and half the time with no precision at all. It follows that the more often he guesses, the smaller his chance of guessing the entire serial number correctly becomes. In fact, even with a serial number of only 10 digits, the probability of counterfeiting a bill of quantum money is 0.00097, that is, 1 success out of every 1,024 attempts. For serial numbers of length 20, a successful outcome is once every 1,048,576 attempts, or 0.0095% of the time.

It is impossible to hack (by way of pattern recognition) this and other related tamper-proof quantum systems [4], and the best a would be counterfeiter can ever do to ascertain the value of a serial number is guess. Further, note that 99.9999% of the time, bankers will know that a counterfeiting attempt has been made! The security of quantum money can be further increased by replacing the protocol or the actual quantum physical system that generates the serial numbers frequently.

Unfortunately, while quantum money is tamper-proof in principle, engineering its implementation is fraught with challenges, though dramatic progress has been made in this area since the beginning of the 21st century. The most promising approach to implementing quantum money is via the quantum systems known as photons, or units of light (which are fundamentally also wave-like, as per the "weirdness" of quantum mechanics so talked about in media). Photons are already used in many electronic devices, especially smart phones. However, maintaining and manipulating their quantum physical properties essential to implementing quantum monetary protocols is not the main concern for the engineers of these devices. To this end, one needs to fine-tune the use of the photons with respect to the given practical constraints (such as the size of the smart phone or interference with its other functions). And this is where one gets to game the quantum.

Non-cooperative game theory [5] is a well-established field that has seen remarkable success in applications to different disciplines such as economics, politics, and evolutionary biology. Playing games as simple as tic-tac-toe or as complicated as poker or chess may appear to the uninitiated to be based on guess work or just luck. However, upon taking a closer look, all players taking part in a game, no matter how simple or complicated, exhibit a certain "rational" behavior. That is, the players look to maximize their payoffs, where the payoffs may simply be measured in monetary tokens, or more complex measures might be employed such as ideological satisfaction (a willing suicide bomber is completely rational when blowing himself up to achieve, as per his beliefs, instant salvation). Broadly speaking, games are categorized as zero-sum, which are strictly competitive in the sense that one player's "meat" is the other player's "poison", and non-zero-sum where players can benefit from a more relaxed notion of competition.

A standard example of a non-cooperative game and one of the most utilized in scientific literature is Prisoner's Dilemma, a non-zero-sum game. Initially transcribed by Merrill Flood and Melvin Dresher [6], this game demonstrates how rational behavior of the players can produce outcomes that are not the best possible ones for either of them. The narrative of the game is as follows: assume that there are two criminals, A and B, who get arrested on the same day at the same time, and have no opportunity to agree on a mutually beneficial alibi. The prosecutor offers A and B, separately, two options. The first option is to betray your partner, and if they don't betray you, then you are granted freedom. However, if they betray you, then both of you spend 2 years in prison. The second option is to remain silent, and if your partner remains silent as well, both of you spend only one year in prison. However, if your partner betrays you, he will be able to walk free, and you will serve 3 years in prison. These options are summarized in Table 1, which demonstrates all possible payoffs for each player's actions as ordered pairs or numbers, with the first entry in a pair being the payoff to player A and the second being that to player B. In this game, each player wants to minimize the time he spends in prison with the best possible payoff being the one where he walks away with no time in prison. But how likely is that to happen?

Table 1- Prisoner's Dilemma Payoffs

A | B	Silent	Betray
Silent	(-1, -1)	(-3, 0)
Betray	(0,-3)	(-2,-2)

Let's examine A's available strategies and find out the best course of action for him. If B stays silent, then A gets 1-year sentence if he stays silent as well. However, if A betrays, then he can walk free! Now let's assume B will betray. Then, if A stays silent, he gets a 3-years sentence. But if A betrays as well, then he gets 2 years, which is still a better outcome than a 3-year sentence. Thus, A concludes that he is better off betraying B in any case. If B follows a similar line of thinking, he will arrive at the same conclusion. Consequently, neither A nor B will unilaterally deviate from the decision to betray, a situation that in game theory is referred to as *Nash Equilibrium* [4]. Hence, they both end up with a 2-year sentence. Of course, this is not the best option available to either player. It would have been ideal for B if A stayed silent and he betrayed A, and vice versa. Furthermore, if both of them remained silent, they would have gotten away with only 1-year sentences. All of these three options are referred to as being *Pareto optimal* [4], an outcome in a game deviating from which makes one player better but leaves at least one other player worse off. In game theory, a social optimum outcome is ideally desired, that is, an outcome that is both Pareto optimal and a Nash equilibrium. This is not the case in Prisoner's Dilemma. In fact, the only Nash equilibrium we see is the one that disagrees with all of the Pareto optimal outcomes. Hence the "dilemma".

Sometimes there is a natural way out of such dilemmas that has been employed since time immemorial: randomization. Including randomization into a game, via tossing of coins or rolling of dice, so long as the original game structure can be recovered when desired, is known as a game-extension. Not only does randomization allow possible resolution of dilemmas, it also guarantees that in the least, a Nash equilibrium will always exist in the extended mixed game [7]. This is the famous theorem of John Nash that earned him the Noble prize in economics. The importance of this theorem being evident when one imagines playing a game like Prisoner's Dilemma and permanently moving from outcome to outcome, much like the never ceasing warfare that marks the tribal culture from around the world. For

Prisoner's Dilemma, it turns out to the case that the mixed version of the game does not solve the dilemma.

Once randomization links physical processes to the theory of non-cooperative games, one has the ability to apply game theory to any physical process so as to optimize it under constraints. The other point of view can be taken as well where one applies physics to the game at hand, that is, the game is implemented or played physically in the real world via a specific physical mechanism. While in most cases this distinction may be moot, there are cases, in particular when one considers the interplay between game theory and quantum physics, where delineating the two points of view can be crucial. For instance, for a given channel, there is a capacity limit to the amount of information that can be exchanged in a single transaction, and this limit is known as bandwidth. Each player (sender/receiver) needs to optimize the way the communication channel is utilized in order to guarantee maximum payoff. In this context, payoff refers to the amount of exchanged information. In computer security, there are further payoffs taken into account, such as the possibility of eavesdropping. This scenario can be modeled as a non-cooperative game, and it is not only applicable to classical communication, but also for communication channels processing information at the quantum level.

Let us return to the game Prisoner's dilemma. In 1999, Eisert et al. [8] presented a quantum physical implementation of this game and showed that the dilemma, while persisting in the mixed version of the game, vanishes in this quantum one. This is due to the fact that the randomization afforded by the strictly quantum realm is of a higher-order than that afforded by the "classical" physical realm. This remarkable feature is referred to as *quantum entanglement*, a physical characteristic that has no counterpart in the classical domain, and it allows one to create correlations between quantum objects that are stronger and remain in place over cosmic time scales and distances. This means that two photons can be created in an entangled state on Earth and then one of them can be sent to Mars, but information gathered about the one of Earth instantaneously produces precise information about the photon on Mars. Aside from this dramatic property, quantum entanglement can clearly break dilemmas in non-cooperative games!

In addition to the dramatic feature of allowing players to break free of dilemmas, what are other benefits of gaming the quantum? Let us go back to the example of quantum money. While theoretically a perfect solution to the problem of tamper-proof currency, its practical implementation requires that the quantum physical system and the protocol used (to gain information about one of the conjugate pairs) should all perform optimally and therefore should interface with each other optimally under several natural constraints. A complete understanding of these constraints is possible in the form of Nash equilibrium or optimal outcomes in the game model for quantum money. Once achieved, stakeholders can choose the technology platform that comes closest to realizing these outcomes. From an investment in technology point of view, gaming the quantum is not an option but in fact, a necessity.

Finally, while much work has been done in gaming the quantum, or what has come to be known as the theory of *quantum games* [9] in the scientific literature, hard mathematical results in the spirit of Nash's work on the existence of equilibrium in games can be found in [10] for the case where randomization is utilized within a quantum system. For the case where purely quantum physical features are of interest, results pertaining to Nash equilibrium have only just appear in [11]. Not only does much scientific work remains to be done in the

theory on quantum games by up and coming scientific minds, but their applications to the emerging quantum technologies niche remains terra incognita.

References:

[1] W. N. Goetzmann, K. Geert Rouwenhorst (1 August 2005). *The Origins of Value: The Financial Innovations that Created Modern Capital Markets.* Oxford University Press. p. 94. ISBN 978-0-19-517571-4.

[2] S. Wiesner, *Conjugate Coding*, ACM SIGACT News - A special issue on cryptography, vol. 15, pp. 77–78, 1983.

[3] Heisenberg, W. (1927), *Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik*, Zeitschrift für Physik (in German), 43 (3–4): 172–198, Bibcode:1927ZPhy...43..172H.

[4] B. P. Williams, K. A. Britt, and T. S. Humble, *Tamper-Indicating Quantum Seal* , Phys. Rev. Applied **5**, 014001, 4 January 2016.

[5] K. Binomre, *Playing for Real*, Oxford University Press; 1 edition, March 29, 2007.

[6] Kuhn, Steven, *Prisoner's Dilemma*, The Stanford Encyclopedia of Philosophy (Spring 2017 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/spr2017/entries/prisoner-dilemma/>.

[7] J. F. Nash, *Equilibrium Points in n-Person Games*, Proceedings of the National Academy of Sciences Jan 1950, 36 (1) 48-49; DOI:10.1073/pnas.36.1.48

[8] J. Eisert, M. Wilkens, M. Lewenstein, *Quantum Games and Quantum Strategies* Phys. Rev. Lett. 83 (1999) 3077–3080.

[9] F. S. Khan, N. Solmeyer, R. Balu, T. S. Humble, *Quantum Games: A Review of the History, Current State, and Interpretation*, Quantum Information Processing (2018) 17: 309. https://doi.org/10.1007/s11128-018-2082-8.

[10] D. A. Meyer, *Quantum Strategies*, Phys. Rev. Lett. 82, 1052 – Published 1 February 1999.

[11] F. S. Khan, T. S. Humble, *Nash Embedding and Equilibrium in Pure Quantum States*, to appear in Springer Lecture Notes on Computer Science as Proceedings of the first Quantum Technology and Optimization Problems conference, 2019.